Informationssäkerhetspolicy

Denna policy innehåller Simrishamns kommuns viljeinriktning och övergripande mål för informationssäkerhetsarbetet.

Bakgrund

Information är en av kommunens viktigaste tillgångar och är nödvändig för att utföra kommunens grunduppdrag. Information är också av betydande värde för invånare, näringsliv, besökare och forskning.

Bristande informationssäkerhet kan medföra störningar i samhällsviktiga verksamheter, att information går förlorad, förvanskas eller stjäls. Det kan även medföra ekonomiska förluster och att förtroendet för Simrishamns kommun påverkas negativt.

För att trygga informationsförsörjningen ska kommunen bedriva ett långsiktigt och systematiskt informationssäkerhetsarbete.

Omfattning

Samtliga nämnder och deras verksamheter omfattas av denna informationssäkerhetspolicy som kompletterar övriga styrdokument inom IT, säkerhet och kommunikation.

Samtliga medarbetare, förtroendevalda och extern personal omfattas av policyn och dess tillhörande rutiner.

Med informationstillgångar avses all information oavsett om den behandlas i ett IT-system, förekommer på ett papper, i ett anteckningsblock, i arkiv, eller som ett samtal i korridoren eller i telefon. Även film, ljud och bild omfattas av informationssäkerhetsbegreppet.

Informationssäkerhet

Informationssäkerhet kan delas upp i två delar. Den administrativa säkerheten består av styrning, organisation, roller och ansvar, liksom regelverk, processer och systematik. Den tekniska säkerheten är den delen som generellt beskrivs som IT-säkerhet. Här återfinns nätverk, servrar, arbetsstationer, hård- och mjukvara samt serverrum och utrymme för reservkraft, säkerhetskopior etcetera.

Informationssäkerhet handlar om att skapa och upprätthålla lämpliga rutiner och skydd av information utifrån tre aspekter:

- **Tillgänglighet –** Att information är tillgänglig i skälig och förväntad utsträckning och inom rimlig tid.
- **Riktighet –** Att informationen inte kan förändras av obehöriga, av misstag eller på grund av störningar i funktion/system. Informationen ska vara tillförlitlig, korrekt och fullständig.
- **Konfidentialitet –** Att information inte tillgängliggörs eller avslöjas till obehörig.

Övergripande målsättning

En god informationssäkerhet syftar till att säkra en effektiv informationsförsörjning och att undgå fel som påverkar möjligheterna att bedriva en ändamålsenlig verksamhet. Arbetet med informationssäkerhet ska vara systematiskt och långsiktigt. Genom att säkerställa en god nivå av systematiskt informationssäkerhetsarbete möjliggörs att lagkrav efterföljs, kritisk verksamhet upprätthålls, informationsläckage förhindras, kontroll av kostnader uppnås och förtroendet för kommunens tjänster och varumärke skyddas. Med rätt informationssäkerhet uppnås hög kvalitet.

Organisation, roller och ansvar

Grundprincipen är att ansvaret för informationssäkerheten följer det ordinarie verksamhetsansvaret. Detta gäller från kommunledningen till den enskilde medarbetaren och innebär att den som är ansvarig för en viss verksamhet också är ansvarig för informationssäkerheten inom verksamhetsområdet. Kommunens informationssäkerhets-ansvarige och övriga som arbetar specifikt med säkerhet, IT-säkerhet eller andra relaterade frågor fungerar som stöd till kommunens verksamheter att fullfölja sitt ansvar.

Ledningen i form av kommunfullmäktige, kommunstyrelse och nämnderna har det yttersta ansvaret för informationssäkerheten i den verksamhet som bedrivs inom respektive verksamhetsområde.

Varje chef, oavsett nivå, ansvarar för informationssäkerheten inom sin verksamhet. Det åligger chefer att tillse att deras medarbetare har ett säkerhetsmedvetande och tillräcklig förståelse och kunskap för att en tillräcklig informationssäkerhet kan uppnås i verksamheten.

Systemägare är den vars budget belastas av kostnader för informationssystemet. Systemägaren ansvarar för införande, förvaltning och avveckling av de egna informationssystemen enligt uppsatta mål och ansvarar för att systemsäkerhetsanalyser för de egna informationssystemen genomförs.

Systemförvaltare utses av systemägaren och ansvarar, i samverkan med IT-enheten, för den dagliga driften och förvaltningen av aktuellt informationssystem.

IT-enheten samordnar arbetet med säkerheten i Simrishamns kommuns IT-miljö och har tillsynsansvar för att IT-miljön är tillförlitlig och motsvarar interna och externa krav.

Informationssäkerhetsansvarig har det övergripande och strategiska ansvaret att leda, utveckla och samordna informationssäkerhetsarbetet. Informationssäkerhetsansvarig ska arbeta i samråd med säkerhetschefen och IT-chefen.

Arkivarien har tillsynsansvar för att informationen hanteras enligt bestämmelser i tryckfrihetsförordningen, arkivlagen och offentlighets- och sekretesslagen samt att kommunens interna styrdokument rörande informationens långsiktiga hantering och bevarande.

Alla medarbetare har ett ansvar att följa Simrishamns kommuns informationssäkerhetspolicy och rutiner. Medarbetare har också ett ansvar att vara uppmärksam på brister och incidenter rörande informationssäkerheten samt rapportera sådana till närmsta chef och IT-helpdesk.

Dataskyddsombudet har sakkunskap om lagstiftning och praxis om dataskydd. Rollen är självständig, rådgivande och övervakande så att Dataskyddsförordningen följs.

Uppföljning

Efterlevnaden av informationssäkerhetspolicyn ska följas upp regelbundet.

Informationssäkerhetsansvarig ska årligen rapportera läge och status gällande informationssäkerhet till kommundirektör och kommunstyrelsen. Särskilda skäl, som till exempel allvarliga incidenter, brister eller behov, kan motivera ytterligare rapportering.